STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

1.0. PURPOSE

This section contains requirements for contractor implementation of the HHS Privacy *Rule* within the context of the DoD Health Information Privacy Regulation (DoD 6025.*18*-R), the DoD Privacy Program (DoD 5400.11-R), the Privacy Act of 1974 (Public Law 93-579, 5 U.S.C. 552a), as amended, and other applicable laws and regulations. The following provides an outline of the organization of this section:

- Paragraph 1.0. Background and HHS Privacy *Rule* relationships to other regulations and laws
- Paragraph 2.0. HHS Privacy *Rule* requirements applicable to covered entities
- Paragraph 3.0. Contractor relationships to the TRICARE Health Plan
- Paragraph 4.0. TRICARE Health Plan and Contractor Objectives
- Paragraph 5.0. HIPAA Privacy Requirements for Contractors

1.1. Background And Provisions

The Standards for Privacy of Individually Identifiable Health Information *rule* is the second *rule* associated with the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Department of Health and Human Services (HHS) published the final privacy *rule* on December 28, 2000, which amended 45 CFR Subtitle A, Subchapter C, Part 160 and added Part 164, Subpart E, which will be referred to as the "Standards for Privacy of Individually Identifiable Health Information Final Rule" or "Final Rule," or the "HHS Privacy *Rule*, "or "*Rule*." The HHS Privacy *Rule* became effective on April 14, 2001. *In addition, HHS published modifications to the Privacy Rule on August 14, 2002. Compliance with the requirements of the Final Rule and the modifications to the Final Rule is mandated by April 14, 2003.*

1.2. Compliance Date

Compliance with the *Rule* is required no later than April 14, *2003*.

1.3. Applicability

The HHS Privacy *Rule* applies to health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in 1173(a)(1) of the Social Security Act (covered transactions). The

HHS Privacy *Rule* applies to health plans, health care clearinghouses, and health care providers who use and disclose protected health information. The *Rule* refers to health plans, health care clearinghouses, and health care providers as "covered entities". In the following paragraphs, TRICARE is referred to as the covered entity. The contractors are "business associates" of TRICARE. The *Rule* specifically names the health care program for active duty military personnel under Title 10 of the United States Code and the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) a defined in 10 U.S.C. 1072(4), as health plans.

1.4. HHS Privacy *Rule* Relationship To Existing Federal And State Laws And Federal Regulations

The Privacy Act of 1974 and the DoD Privacy Program Regulation, will be interpreted in a manner that will make them compatible with the HHS Privacy *Rule* and the DoD Health Information Privacy Regulation. If a regulation or law mandates a particular action, that regulation or law will take precedence over a regulation that makes a particular action discretionary. Further, the more specific regulation or law will take precedence over the more general regulation or law. Where a determination must be made as to the applicability of a privacy requirement, the general rule is that the more restrictive requirement will be applied.

The preamble of the HHS Privacy *Rule* states,

> "When a covered entity is faced with a question as to whether the privacy regulation would prohibit the disclosure of protected health information that it seeks to disclose pursuant to a federal law, the covered entity should determine if the disclosure is required by that law. In other words, it must determine if the disclosure is mandatory rather than merely permissible. If it is mandatory, a covered entity may disclose the protected health information pursuant to §164.512(a), which permits covered entities to disclose protected health information without an authorization when the disclosure is required by law. If the disclosure is not required (but only permitted) by the federal law, the covered entity must determine if the disclosure comes within one of the provisions for permissible disclosures, the covered entity must obtain an authorization from the individual who is the subject of the information or de-identify the information before disclosing it. If another federal law prohibits a covered entity for using or disclosing information that is also protected health information, but the privacy regulation permits the use or disclosure, a covered entity will need to comply with the other federal law and not use or disclose the information."

1.4.1. The Privacy Act Of 1974 And The DoD *Health Information* Privacy Regulation

The Military Health System (MHS), TRICARE, and its contractors are subject to the Privacy Act of 1974 and the DoD Privacy Program Regulation. The Privacy Act and the DoD Privacy Program Regulation permit the disclosure of information for reasons compatible with the purposes for which the information was collected. These uses and conditions or reasons for disclosures of information, otherwise referred to as "routine uses,"

must be identified and published in the Federal Register. Routine uses are defined by the agency and are, by definition, discretionary. Where a routine use conflicts with mandatory requirements under the HHS Privacy Regulation, the routine use must be interpreted or applied in a manner that complies with the HHS Privacy *Rule* requirements.

1.4.2. Freedom Of Information Act (FOIA)

The FOIA, 5 U.S.C. 552, requires the federal government to disclose several types of information upon the request of any person. Uses and disclosures required by FOIA fall under §164.512(a) of the HHS Privacy *Rule* which allows for uses and disclosures required by law. The HHS Privacy *Rule* does not change the established policies and procedures for the contractor toward FOIA requests, as specified in Chapter 1, Section 5.

1.4.3. State Laws

1.4.3.1. The general rule set forth in the HHS Privacy *Rule* states that any standard, requirement, or implementation guideline adopted in the privacy rule that is contrary to state law will preempt that state law unless one of the privacy rule exceptions apply. In other words, federal privacy regulations adopted pursuant to the HIPAA privacy rule, set the floor of minimal privacy requirements that must be met by covered entities in all states. States are permitted to enforce requirements that exceed the federal minimum.

1.4.3.2. Generally, state laws pertaining to health care are not applicable to health care programs and activities of the Department of Defense (DoD). However, there are circumstances when DoD procedures require DoD components (including contractors) to follow state law. In those cases DoD components will follow state law. For example, state law (where treatment is provided) will be applied to cases involving the disclosure of protected health information (PHI) about a minor to authorized persons (i.e., parent, guardian, etc.).

1.4.3.3. Paragraph C2.4. of the DoD Health Information Privacy Regulation provides guidance regarding the preemption of state law.

> "In general, the HHS *Rule* establishes rules, exceptions, and procedures governing the determination of the preemption of state law by the HHS regulation. As a general rule, a standard, requirement, or implementation specification adopted under the HHS regulation that is contrary to a provision of State law preempts the provision of State law. *Exceptions* to this general rule include the circumstance in which the provision of State law relates to the privacy of health information and is more stringent than a standard requirement, or implementation specification adopted under the HHS *Rule*. Exceptions also include circumstances in which the provision of State law, including State procedures established under such law, as applicable, provide for the reporting of disease or injury, child *or domestic* abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention."
>
> "As a general rule, State laws pertaining to health care are not applicable to health care programs and activities of the Department of Defense. However, there are some matters concerning which

Department of Defense rules and procedures call for DoD components to follow State law. For example, in cases involving disclosure of protected health information about a minor to a parent, guardian, or person acting in loco parentis of such minor, the State law of the state where the treatment is provided *shall* be applied. In any other case in which there is a conflict between this regulation [DoD Health Information Privacy Regulation] and State law, this regulation [DoD Health Information Privacy Regulation] *shall* apply, unless DoD rules, procedures, or other applicable policy call for DoD components to follow State law with respect to the matter at issue."

1.4.4. The Alcohol, Drug Abuse, And Mental Health Administration Reorganization Act (ADAMHA)

The Alcohol, Drug Abuse, and Mental Health Administration Reorganization Act, Public Law 102-321 (enacted July 10, 1992, with an effective date of October 1, 1992) (42 U.S.C. Section 290dd-2) places specific requirements upon Federal agencies (and their agents) regarding the confidentiality and disclosure of records and the identity, diagnosis, prognosis or treatment of any beneficiary in connection with drug abuse, alcoholism or an alcohol abuse program. The HHS Privacy *Rule* permits a health care provider to disclose information in a number of situations that are not permitted under the substance abuse regulation (ADAMHA). For example, disclosures allowed without patient authorization under the HHS Privacy *Rule* for law enforcement, judicial and administrative proceedings, public health, health oversight, directory assistance, and as required by other laws would generally be prohibited under the substance abuse statute and regulation. However, because these disclosures are discretionary and not mandatory, there is no conflict. A covered entity would not be in violation of the HHS Privacy *rule* for not disclosing this information and for complying with ADAMHA requirements.

1.5. Compliance And Enforcement

Violations by the covered entity of the HHS Privacy *Rule* are punishable by civil monetary penalties of up to $100 for each violation. In addition, a wrongful use or disclosure of protected health information is subject to criminal penalties of up to a $250,000 fine, 10 years imprisonment, or both.

2.0. HIPAA PRIVACY STANDARDS/IMPLEMENTATION SPECIFICATIONS

The relevant segments of the HHS Privacy *Rule* applicable to contractors are summarized below. This summarization is not intended to capture all the details associated with the HHS Privacy *Rule* but to offer general guidance for assistance in implementing requirements.

2.1. General Uses And Disclosures Of Protected Health Information

The HHS Privacy *Rule* states that personally identifiable health information may not be used or disclosed except for specifically permitted uses. One set of rules applies to the use and disclosure of protected health information (PHI) for treatment, payment or health care operations. Payment and health care operations directly relate to the functions performed by the contractor (Chapter 24, Addendum A provides complete definitions of these terms).

- Payment includes: collection of premiums; reimbursement for the provision of health care; determinations of eligibility or coverage; billing; claims management; collection activities; medical necessity reviews; utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services.

- Health care operations includes: quality assessment activities; case management and care coordination; evaluating provider performance; provider certification and credentialing activities; medical review and auditing, including fraud and abuse detection and compliance programs; business management and general administrative activities.

2.1.1. The following are required disclosures of protected health information:

- To an individual as required under Sections 164.524 and 164.528; and

- When required by the Secretary of HHS to investigate or determine the covered entity's compliance with the HHS Privacy *Rule*.

2.1.2. The following are permitted uses and disclosures for which an authorization or opportunity to agree or object is not required:

- Required by law
- Public health activities
- Victims of abuse, neglect or domestic violence
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement
- Victims of a crime
- Decedents (coroners, medical examiners, funeral directors)
- Cadaveric organ, eye or tissue donation
- Research purposes
- Avert a serious threat to health and safety
- Specialized government functions
- Workers compensation

2.1.2.1. For armed forces personnel, the privacy rule does not change the 'routine use' provision as described in Chapter 1, Section 5. The HHS Privacy *Rule* (164.512 (k)(1)(i)) states that: "a covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if appropriate military authority has published by notice in the Federal Register the following information:

- Appropriate military command authorities; and

- The purposes for which the protected health information may be used or disclosed."

The DoD Health Information Privacy Regulation identifies the appropriate military command authorities as the following:

- "All commanders who exercise authority over an individual who is a member of the Armed Forces, or other person designated by such a commander to receive protected health information in order to carry out an activity under the authority of the commander.

- The Secretary of Defense, the Secretary of the Military Department responsible for the armed force of which the individual is a member, or the Secretary of Transportation in the case of a member of the Coast Guard when it is not operating as a service in the Department of the Navy.

- Any official delegated authority by a Secretary listed in [the previous bullet] to take an action designed to assure the proper execution of the military mission."

The DoD Health Information Privacy Regulation specifies the purposes for which the protected health information who is a member of the Armed Forces may be used or disclosed as follows:

- "To determine the member's fitness for duty, including but not limited to the member's compliance with standards and all other activities carried out under the authority of DoD Directive 1308.1, "DoD Physical Fitness and Body Fat Program," July 20, 1995, DoD Directive 1332.38, "Physical Disability Evaluation," November 14, 1996, and similar requirements.

- To determine the member's fitness to perform any particular mission, assignment, order, or duty, including compliance with any actions required as a precondition to performance of such mission, assignment, order, or duty.

- To carry out activities under the authority of DoD Directive 6490.2, "Joint Medical Surveillance," August 30, 1997.

- To report on casualties in any military operation or activity in accordance with applicable military regulations or procedures.

- To carry out any other activity necessary to the proper execution of the mission of the Armed Forces."

2.1.3. Other Privacy Practices Concerning Uses And Disclosures include:

2.1.3.1. Minimum Necessary Rule

The HHS Privacy *Rule* delineates the standards and implementation specifications for the minimum necessary rule at §164.502(b) and §164.514(d). The regulation states the following: "When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit the protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

2.1.3.1.1. The minimum necessary rule is similar to the Privacy Act of 1974's rule of "relevant and necessary" and "need to know." For example, the contractor shall continue to

limit requests to and from providers for PHI to the minimum necessary to accomplish utilization and quality management, claims processing, appeals/hearings functions, etc.

2.1.3.1.2. The minimum necessary rule does not apply to the following types of uses and disclosures, as referenced in the HHS Privacy *Rule*, §164.502(b)(2):

- Disclosures to or requests by a health care provider for treatment purposes;
- Uses or disclosures made to the individual;
- Uses or disclosures made pursuant to an authorization under the HHS Privacy *Rule*, §164.508;
- Disclosures made to the Secretary of HHS in accordance with the HHS Privacy *Rule*, subpart C of part 160;
- Uses or disclosures required by law, as described by §164.512 (a); and
- Uses or disclosures that are required for compliance with applicable requirements of the HHS Privacy *Rule*.

2.1.3.2. Whistle-Blower Provision

The HHS Privacy *Rule* provides protection to the covered entity for the good faith whistle-blower action of a member of its workforce or a business associate. As stated at §164.502(j)(1), "The covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information"... to a health oversight agency or public health authority, an appropriate health care accreditation organization, or an attorney, for the purpose of determining the whistle-blower's legal options. Whistle-blowers are not subject to the "minimum necessary" provisions.

2.1.3.3. Disclosures By Workforce Members Who Are Victims Of A Crime

The HHS *Rule* states in §164.502(j)(2) that, "a covered entity is not considered to have violated the requirements of this subpart [minimum necessary provision], if a member of its workforce who is a victim of a criminal act discloses protected health information to a law enforcement official, provided that: (i) the protected health information disclosed is about the suspected perpetrator of the criminal act; and (ii) the protected health information disclosed is limited to the information listed under §164.512(f)(2)(i)."

2.1.3.4. Personal Representatives

A covered entity and its business associates will treat a personal representative as the individual, if, "…a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative… with respect to protected health information relevant to such personal representation" as stated in the HHS Privacy *Rule* §164.502 (g)(1).

2.1.3.4.1. Unemancipated Minors

The HHS Privacy *Rule* states in §164.502 (g)(3): "If under applicable law, a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative." However, a personal representative may not serve as the minor person's personal representative, and the minor has the authority to act as an individual with respect to protected health information if:

- The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative.

- The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or

- A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between the contractor and the minor with respect to such health care service."

The HHS Privacy *Rule* at §164.502 (g)(3)(ii), states the following: "Notwithstanding the provisions of paragraph (g)(3)(i) [includes bullet statements above] of this section:

- (A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with §164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis.

- (B) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with §164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis.

- (C) Where the parent, guardian, or other person acting in loco parentis, is not the personal representative under paragraph (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under §164.524 to a parent, guardian, or other person acting in loco parentis, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

2.1.3.4.2. Deceased Individuals

According to §164.502 (g)(4) of the HHS Privacy *Rule*: "If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative… with respect to the deceased individual's protected health information." Since the Privacy Act of 1974 and the DoD Health Information Privacy Regulation are silent on the protected health information of deceased individuals, this is new guidance.

2.1.3.4.3. Abuse, Neglect, Endangerment Situations

According to §164.502(g)(5) of the HHS Privacy *Rule*: "Notwithstanding a State law…to the contrary, the covered entity may elect not to treat a person as the personal representative if:

- The covered entity has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by such person, or treating such person as the personal representative could endanger the individual; and

- The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative."

2.2. Authorizations For Uses And Disclosures

2.2.1. The HHS Privacy *Rule* at §164.508(a) states, "Except as otherwise permitted or required by this subchapter [Subpart C, Compliance and Enforcement] a covered entity may not use or disclose protected health information without an authorization that is valid under this section." The HHS Privacy *Rule* at §164.508(a)(2) identifies two specific instances when an authorization must be obtained from the individual: for any use or disclosure of psychotherapy notes (with certain exceptions) and for any use or disclosure of protected health information for marketing. The HHS Privacy *Rule* at §164.508 (a)(2) states: …a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except: (i) To carry out the following treatment, payment, or health care operations, (A) Use by the originator of the psychotherapy notes for treatment; (B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling; or (C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual." Additional exceptions include: uses or disclosures required by the Secretary, permitted by law, for health oversight activities, for coroners and medical examiners, to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and released to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat (HHS Privacy *Rule*, §164.502(a)(ii), §164.512(a), §164.512(d), §164.512(g)(1), §164.512 164.512(j)(1)(i)). According to the HHS Privacy *Rule* at §164.508(b)(5), individuals have the right to revoke an authorization at any time, except to the extent the covered entity has already taken action based on the authorization.

2.2.2. Revocations Of Authorizations

The HHS Privacy *Rule*, §164.508(b), allows an individual to revoke an authorization at any time provided that it is in writing. A covered entity that knows of an individual's revocation must stop making uses and disclosures pursuant to the authorization to the greatest practical extent. However, the covered entity may continue to use and disclose the individual's protected health information only to the extent the covered entity has taken action in reliance on the authorization.

2.2.3. Psychotherapy Notes

A patient's authorization is required for the use and disclosure of psychotherapy notes (see Chapter 24, Addendum A for definition) except for use by the originator of the notes for treatment, or for use or disclosure by the covered entity for its own mental health training programs, and use or disclosure by the health plan to defend a legal action or other proceeding brought by the individual. If during the appeal process it is determined that psychotherapy notes are necessary, and the appeal is filed by someone other than the beneficiary or the beneficiary's appointed personal representative, an authorization by the beneficiary releasing the psychotherapy notes is required. To meet the HIPAA definition of psychotherapy notes, the information must be maintained separately from the rest of the medical record. Progress notes, treatment plans, prognoses, etc., are not included in the definition of psychotherapy notes and can be used by the health plan for payment and healthcare operations without an authorization.

2.2.4. Marketing

A covered entity must obtain an authorization from the individual for any use or disclosure of protected health information for marketing activities (see Chapter 24, Addendum A for a complete definition), unless the form of communication is face to face or a promotional gift of nominal value provided by the covered entity. An authorization is not required for the covered entity's communication to eligible beneficiaries regarding their program benefits. For example, an authorization is not required for contractor communications to beneficiaries regarding TRICARE program benefits. Such activities do not generally meet the HIPAA definition of "marketing." The contractor shall continue to comply with the marketing requirements outlined in the Chapter 12, Section 1.

2.3. Other Requirements Relating To Uses And Disclosures Of PHI

2.3.1. De-Identified Data

According to §164.514 (a) of the HHS Privacy *Rule*, "Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information... (b) A covered entity may determine that health information is not individually identifiable, only if: (1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable…. or (2)(i) ….identifiers [as listed in the privacy rule] of the individual or of relatives, employers, or household members of the individual are removed." Chapter 24, Addendum A lists the identifiers to be removed. The covered entity may use and disclose de-identified data without a consent or authorization, since the data is

no longer individually identifiable information. The covered entity may not disclose protected health information in a de-identified format that could later be re-identified. Reports containing de-identified information are not subject to the HHS Privacy *Rule*.

2.3.2. Individual Rights

The privacy rule requires covered entities to implement administrative standards to ensure compliance with privacy standards. The covered entity must not require individuals to waive their rights as a condition of the provision of treatment, payment, or enrollment in the health plan or eligibility of benefits. Following is a listing of those standards identified in the HHS Privacy *Rule* (§164.520, §164.522, §164.524, §164.526, §164.528, and §164.530):

- The covered entity must provide individuals the ability to inspect and copy PHI;
- The covered entity must provide individuals the ability to request a restriction on the use and disclosure of PHI;
- The covered entity must provide individuals the ability to request to receive confidential communications by alternative means or at an alternative location;
- The covered entity must provide individuals the ability to request amendment to their PHI;
- The covered entity must provide individuals the ability to request to receive an accounting of certain disclosures that have been made of their PHI; and
- The covered entity must provide individuals the ability to file complaints of any alleged violations of privacy rights.

2.3.3. Right To Access

The HHS Privacy *Rule* (§164.524(a)) states "…an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set." Chapter 24, Addendum A provides the definition of the designated record set. The individual must be granted access to their protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the individual and the covered entity. If the individual requests a copy of their protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee.

2.3.3.1. The HHS Privacy *Rule* specifies at §164.524(a)(1) that an individual has no right of access to the following information:

- Psychotherapy notes;

- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

- Protected health information maintained by a covered entity that is subject to the Clinical Laboratory Improvements Amendments (CLIA) to the extent of the provision of access to the individual would be prohibited by law; or is a laboratory exempt from CLIA.

2.3.3.2. Access can be denied in the following circumstances (HHS Privacy *Rule*, §164.524(d)):

- When the access is reasonably likely, according to a licensed professional, to endanger the life or physical safety of the individual or another person. This includes situations where the individual exhibits suicidal or homicidal tendencies;

- When the protected health information makes reference to another person (unless such other person is a health care provider) and the access requested is reasonably likely to cause substantial harm to such other person; or

- When the request for access is made by the individual's personal representative and the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

2.3.4. Right To Notice

In accordance with the HHS Privacy *Rule*, §164.520 (a), all Military Health System and TRICARE beneficiaries have a right to adequate notice of the uses and disclosures of protected health information that may be made and of the individual's rights and TRICARE's or their health care provider's legal duties with respect to that information. All Military Health System and TRICARE beneficiaries, who are provided direct health care treatment by a TRICARE network or non-network provider, should receive a Notice of Privacy Practices from that health care provider. The Military Health System and TRICARE health plan will use the "Military Health System Notice of Privacy Practices." The Military Health System will ensure the dissemination of this notice prior to the compliance date.

2.3.5. Right To Request Restriction Of Uses And Disclosures

The HHS Privacy *Rule*, §164.522(a), provides the individual the right to request a restriction on the use and disclosure of protected health information about the individual to carry out treatment, payment, and healthcare operations; and disclosures to family and friends involved in the individual's care. TMA's policy is that health care providers who agree to a restriction on the disclosure of protected health information necessary for payment functions as defined in the HHS Privacy *Rule* may result in a denial of payment.

2.3.6. Right To Receive Confidential Communications.

The HHS Privacy *Rule* (Section 164.520) states "a health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive

communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual…". The covered entity may consider the administrative difficulty of complying with the request when deciding whether or not to accommodate the request. The HHS Privacy *Rule* at §164.522(b)2.ii states "A covered entity may condition the provision of a reasonable accommodation on: A. When appropriate, information as to how payment will be handled; and B. Specification of an alternative address or other method of contact. "

2.3.7. Right To Accounting Of Disclosures.

The HHS Privacy *Rule* at Section 164.528 (a)(1), states, "An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

- (i) To carry out treatment, payment and healthcare operations as provided in §164.506; [Uses or disclosures to carry out treatment, payment, or health care operations.]
- (ii) To individuals of protected health information about them as provided in §164.502;
- (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in §164.502;
- (iv) Pursuant to an authorization as provided in §164.508;
- (v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in §164.510;
- (vi) For national security or intelligence purposes as provided in §164.512(k)(2);
- (vii) That occurred prior to the compliance date for the covered entity;
- (viii) As part of a limited data set in accordance with §164.514(e); or
- (ix) To correctional institutions or law enforcement officials as provided in §164.512(k)(5)."

2.3.8. Right To Request Amendment Of Protected Health Information

The HHS Privacy *Rule* at §164.526 (b)(1) states "The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in a designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements." The *Rule* at §164.526(b) indicates that an individual has the right to request an amendment to their

protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

2.4. The following standards and implementation specifications as described in the HHS Privacy *Rule*, §164.530, require certain actions by covered entities.

2.4.1. Personnel Designations

"A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. A covered entity must designate a contact person or office who is responsible for receiving complaints…and who is able to provide further information about matters covered by the notice required by §164.520."

2.4.2. Training

"A covered entity must train all members of its workforce with respect to protected health information…as necessary and appropriate for the members of the workforce to carry out their function within the covered entity."

2.4.3. Safeguards

"A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications, or other requirements…" In addition, "a covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure."

2.4.4. Complaints

"A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures or its compliance with such policies and procedures…" The following provides additional guidance:

2.4.4.1. The contractor shall inform any person, who believes TRICARE, its business associates, or any providers providing health care to TRICARE beneficiaries are not complying with the HIPAA regulations, that he or she may file a complaint with the contractor, MTF Privacy Officer, TMA Privacy Officer, or with the Secretary of the U.S. Department of Health and Human Services (HHS). The complainant need not notify the contractor or TMA Privacy *Officer* prior to filing the complaint with the Secretary of HHS.

2.4.4.2. Complaints relating to HHS Privacy *Rule* must be filed within 180 days of when the complainant knew or should have known that the act or omission occurred, unless the HHS Secretary for good cause shown waives this time limit.

2.4.5. Sanctions, Mitigation, Refraining From Intimidating Or Retaliatory Acts

"A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures… A covered entity shall mitigate, to the extent practicable, any harmful effect that is known to the covered entity

of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate." The covered entity must not sanction workforce members or business associates for whistle blowing activity provided the disclosure was made in good faith that the covered entity engaged in conduct that is unlawful or otherwise violates professional or clinical standards. The covered entity also is prohibited from intimidation, threats, coercion, discrimination, or retaliation against any whistle-blower acting in good faith.

2.4.6. Waiver Of Rights

"A covered entity may not require individuals to waive their rights…under this regulation…as a condition of the provision of treatment payment, enrollment in a health plan, or eligibility for benefits."

2.4.7. Policies and Procedures

"A covered entity must implement policies and procedures with respect to protected health information that...comply with the standards, implementation specifications, or other requirements of this subpart [HHS Privacy *Rule*]." A covered entity must make changes to their policies and procedures as necessary to comply with changes in the law.

2.4.8. Documentation

The HHS Privacy *Rule* states at §164.530(j) (1), "A covered entity must: (i) Maintain the policies and procedures...in written or electronic form; (ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and (iii) If an action, activity, or designation, is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation...(2) A covered entity must retain documentation...for six years from the date of its creation or the date when it last was in effect, whichever is later."

2.4.9. Transitions

The covered entity may honor an authorization or other express legal document obtained from an individual permitting the use and disclosure of protected health information prior to the compliance date (HHS Privacy *Rule*, §164.532). However, new requests for use or disclosure of protected health information received on April 14, 2003 and after must meet the core elements and requirements for authorizations as specified in the HHS Privacy *Rule*.

3.0. CONTRACTOR RELATIONSHIPS TO TRICARE HEALTH PLAN

The HHS Privacy *Rule* specifically names the health care program for active duty military personnel under Title 10 of the United States Code and the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) as defined in 10 U.S.C. 1072(4), as health plans. Prime contractors and any of their subcontractors must comply as business associates with the HHS Privacy *Rule* in the same manner as the TRICARE health plan. Network providers are not considered business associates of the TRICARE health plan, and shall comply with the provisions of the HHS Privacy *Rule* as covered entities.

3.1. Business Associates

The HHS Privacy *Rule* states at §164.502(e): "A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity must document the satisfactory assurances...through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of §164.504(e)." Contractors are considered a business associate of the TRICARE health plan. In §164.504(e)(ii) the Regulation states: "A covered entity is not in compliance with the standards in §164.502 (e), [Disclosures to Business Associates], and paragraph (e) of this section [Business Associate Contracts], if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

- A. Terminated the contract or arrangement, if feasible;
- B. If termination is not feasible, reported the problem to the Secretary"

4.0. TRICARE OBJECTIVES

4.1. The TRICARE health plan and its business associates shall be in full compliance with the HHS Privacy Final Rule no later than April 14, 2003.

4.2. The TRICARE health plan will ensure that contractors establish, update, and document policies and procedures to comply with the HHS Privacy *Rule* standards.

4.3. The TRICARE health plan will ensure that contractors review, revise and conduct workforce training to include the HHS Privacy *Rule*.

4.4. The TRICARE health plan will ensure that contractors designate a privacy official for the implementation and compliance of all applicable Privacy Laws and Regulations.

5.0. HIPAA PRIVACY REQUIREMENTS FOR CONTRACTORS

5.1. Risk Assessments

The contractor shall conduct initial and periodic privacy risk assessments and related ongoing compliance monitoring activities, as applicable. The initial risk assessment shall compare current practices against HHS Privacy *Rule* and DoD Health Information Privacy Regulation directives and TMA Privacy requirements. The contractor shall develop an action plan from identified and prioritized findings to achieve compliance.

5.1.1. The contractor shall submit the initial privacy risk assessment and the accompanying action plan by December 16, 2002, to the Contracting Officer (CO), with copies to the Regional Director, Administrative Contracting Officer (ACO), Contracting Officer Representative (COR), and the TMA Privacy Officer.

5.1.2. The contractor shall conduct no less than one privacy risk assessment every calendar year subsequent to April 14, 2003, and provide a letter of assurance to report the results of their assessment (see Chapter 24, Addendum C). The letter of assurance shall be forwarded by April 14th each year, to the Regional Director, with copies to the Administrative Contracting Officer (ACO), Contracting Officer (CO), Contracting Officer Representative (COR), and the TMA Privacy Officer. If significant discrepancies are identified, the Regional Director may request additional assessments.

5.1.3. The TMA Privacy Officer, in coordination with the Regional Directors, will have primary monitoring and enforcement responsibilities.

5.2. Tracking And Accounting

5.2.1. According to the HHS HIPAA Privacy *Rule's* minimum necessary rule, the contractor shall identify and document those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties. For each person or class of persons identified, the contractor shall document the category or categories of protected health information needed and any conditions appropriate to such access.

5.2.1.1. If the entire medical record is needed to complete a review, claims or appeals/ hearings function, the contractor shall identify and document the circumstances and justification in their policies and procedures.

5.2.1.2. The contractor shall forward privacy requests for non-routine or nonrecurring disclosures to the Regional Director within three working days of receipt of the request. Non-routine or nonrecurring disclosures are any disclosures outside the current routine uses published in the Federal Register under the Privacy Act of 1974 and not covered in the contractor's policies and procedures addressing the HHS Privacy *Rule's* minimum necessary rule. Privacy requests for protected health information shall be made in writing. The Regional Director in consultation with the contractor will forward the request and recommendation within 10 working days of receipt of the request from the contractor to the TMA Privacy Officer. The TMA Privacy Officer will make the final determination as to what information is reasonably necessary to accomplish the purpose for which the disclosure or request is sought.

5.2.2. The contractor shall document privacy complaints received, and retain a case file of all documentation associated with a complaint. These files shall be retained until the end of the calendar year in which it was received plus an additional 6 years. The contractor shall use the existing grievance process and time lines as identified in Chapter 12, Section 9, to provide a process for individuals to make complaints concerning either TMA or the contractor's policies and procedures or its compliance with such policies and procedures or the requirements of the HHS Privacy *Rule*.

5.2.3. All records shall be maintained in accordance with Chapter 2, Records Management.

5.2.4. For access to protected health information under the HHS Privacy *Rule*, the contractor shall ensure all requests for access are in writing. If the contractor grants the request for access, it must inform the individual of the acceptance of the request and provide

the access requested no later than 30 calendar days after receipt of the request. If the contractor is unable to take the requested action within 30 calendar days, the contractor may extend the time for no more than an additional 30 days provided that they notify the individual in writing of the delay and the date by which it will be completed. Only one 30-calendar day extension may be allowed under the HHS privacy *rule*. The contractor shall document receipt of all access requests using a date stamp and maintain an index to record pertinent information and actions. If the contractor determines they will not grant access to the protected health information or the record, they shall forward the request within seven working days from date of receipt to the Regional Director. The contractor shall notify the beneficiary within three working days that their request was forwarded to the Regional Director. The Regional Director will review the request and make a determination within 20 calendar days (50 calendar days for justified delays) of the date of the original request. The Regional Director will notify the individual of denied or approved access determinations and the reason for any denial. If the individual disagrees with the denial determination, the individual may appeal the decision to the TMA Privacy Officer. The contractor shall consider the following when making a determination on charging fees for copying protected health information:

- Charge only reproduction costs,
- Fees will be waived when those costs are under $30, and
- There will be no charge when the copying is for the contractor's or the TRICARE health plan's convenience.

5.2.5. Upon written request from the individual, the contractor shall provide a written accounting of disclosures as allowed under the HHS Privacy *Rule* and the DoD Health Information Privacy Regulation. The HHS Privacy *Rule* requires an accounting of disclosures for the previous 6 years from the date of the request. The contractor shall use existing disclosure accounting processes in place for the Privacy Act of 1974 as identified in Chapter 1, Section 5.

5.2.6. Requesting An Amendment

The contractor shall document the title(s) of the person(s) or office(s) responsible for receiving and processing requests for amendments by individuals.

5.2.6.1. If an individual requests amendment to their protected health information under the Privacy Act of 1974, the request shall be processed in accordance with that law's directions and timeliness standards. The contractor shall continue to use the existing procedures required in Chapter 1, Section 5, to ensure compliance with the Privacy Act of 1974 when considering amendment requests by individuals.

5.2.6.2. If an individual requests an amendment to their protected health information under the HHS Privacy *Rule*, the request shall be processed in accordance with that regulation's standards, implementation specifications and timeliness standards. All amendment requests must be submitted in writing. If the contractor determines to amend the protected health information or record, the amendment shall be completed within 60 calendar days of receipt of request. The contractor shall provide a reason for any extension beyond the 60 calendar days with an estimated date of completion, in writing, to the

individual who made the request with a courtesy copy to the Regional Director. Only one 30 calendar day extension may be allowed under the HHS Privacy *Rule*. The contractor shall document receipt of all amendment requests using a date stamp and maintain an index to record pertinent information and actions. If a determination is made to not amend the protected health information or the record, the contractor shall forward the request to the Regional Director within 20 calendar days from receipt of the request. The Regional Director will review the request and make a determination within 45 calendar days (80 calendar days for justified delays) from the receipt date of the original request. The Regional Director will notify the individual of amendment determinations and the reason for any denial. If the individual disagrees with the denial determination, the individual may appeal the decision to the TMA Privacy Officer. Whoever makes the decision on whether to amend or not is the responsible agent for communicating with the beneficiary regarding their amendment request.

5.2.7. The contractor shall accommodate reasonable requests by individuals to receive communications of protected health information by alternative means or at alternative locations. Requests for confidential communications shall be addressed by the contractor. The contractor shall maintain a log of all requests for alternative communications to include a control number, name and address of individual, date request received, date request was completed, and the requested action.

5.3. Education And Training

5.3.1. Workforce Training

The contractor shall train all workforce members (including, but not limited to, employees, volunteers, trainees, and other persons who conduct, and perform work for the contractor) to carry out their functions with respect to the HHS Privacy *Rule* and the DoD Health Information Privacy Regulation, and on the policies and procedures identified in this section of the Operations Manual.

5.3.1.1. The contractor shall provide workforce training as follows:

- To each member of its workforce no later than April 14, 2003;
- Thereafter, to each new member of the workforce within 30 work days of starting work;
- Subsequent refresher training shall be conducted annually to demonstrate the importance of the Regulation and to ensure the workforce understands the rules, policies, and procedures; and
- Retraining must occur within 30 days for all members of the workforce whose functions are affected by a HHS HIPAA Privacy material change affecting TRICARE or the contractor's policies and procedures.

5.3.1.2. The contractor shall document all training provided to its workforce to include, as a minimum, who received the training on what date.

5.3.2. Education: Beneficiaries And Providers

The contractor shall include instructions on how to obtain the MHS Notice of Privacy Practices with educational materials provided to beneficiaries. General information on the HIPAA privacy requirements shall also be included in existing routine mailings to the beneficiary. The contractor shall respond to all questions regarding the HHS Privacy *Rule* using the following standards: 85% of all requests shall be answered in 10 calendar days of receipt and 100% in 30 calendar days. Questions of a non-routine nature or that require additional assistance to resolve, shall be coordinated with the Military Treatment Facility Privacy Officer for co-located TRICARE Service Centers and to the Regional Directors for all others. (See paragraph 5.4.1. below.)

5.4. *Reports* To TRICARE Management Activity

5.4.1. The contractor shall forward a monthly report to the Regional Director with copies to the TMA Privacy Officer and the Contracting Officer, reporting the beneficiary's name, sponsor's social security number, nature of the complaint, the steps taken to resolve the complaint, the date of the initial complaint, and the expected date of resolution or the date the complaint was resolved. This report shall be sent no later than the 10th calendar day of the month following the month being reported. The contractor shall use the sample report format at Chapter 24, Addendum C. See paragraph 5.3.2. for time lines in responding to beneficiary's complaints.

5.4.2. Requests for a restriction to be placed on communications must be in writing. The contractor shall accept and review submitted restriction requests on protected health information. The contractor shall determine whether or not to grant a restriction request within seven working days of receiving the request. If the restriction request is approved, the contractor shall notify the individual who made the request and the Regional Director. If the restriction is granted, it shall be implemented within seven working days of the date of the decision to grant the request. If denied, the contractor shall notify the individual making the request within seven working days of the decision. Requests for termination of the restriction must be in writing.

5.4.3. The contractor shall accommodate reasonable requests by individuals to receive communications of protected health information to alternative locations or means if the individual clearly states the disclosure of all or part of their protected health information could endanger them. For example, an individual requests that the explanation of benefits concerning particular services be sent to their work place rather than a home address because the individual is concerned that a member of the household might read the explanation of benefits and become abusive towards them.

5.5. Authorizations

5.5.1. The contractor shall use authorizations conforming to the core elements identified in the HHS Privacy *Rule* at §164.508(c), as necessary. The contractor shall obtain a signed authorization for any use and disclosure consistent with the DoD Health Information Privacy Regulation, Chapter 5, and the HHS Privacy *Rule*, §164.508(a). A copy of the signed authorization shall be given to the individual. Authorizations may be revoked upon written request by the individual. See paragraph 5.2.5. for storing and maintaining authorizations and paragraph 2.3.2. on revocations of authorizations.

5.5.2. If the contractor requires the psychotherapy notes, a signed authorization from that individual subject to the exceptions listed at paragraphs 2.3.1. and 2.3.3. shall be obtained. Under the HHS Privacy *Rule*, the contractor shall not release the psychotherapy notes to the individual who is the subject of the notes. However, under the Privacy Act of 1974 case law, the individual may have access to all of their health information, including their psychotherapy notes. Due to such complexities, the contractor shall refer all determinations for release of psychotherapy notes to the TMA Office of General Counsel. The definition of psychotherapy notes is included in Chapter 24, Addendum A.

5.5.3. The contractor shall ensure special report requests using or disclosing individuals' protected health information are included in the HHS Privacy *Rule* definitions of treatment, payment or health care operations. If not, an authorization from the beneficiary is required.

5.5.4. HIPAA authorizations acquired or used by the contractor in the development and processing of claims or required for other contractor functions, such as fraud and abuse, shall be stored and maintained with the appropriate record categories described in Chapter 2.

5.6. Notice Of Privacy Practices

5.6.1. Annually, the contractor shall notify individuals of the availability of the notice and how to obtain the notice. This communication shall occur only through beneficiary education vehicles permitted within existing contract limitations and requirements. No additional or special marketing or beneficiary education campaigns are required.

5.6.2. The contractor shall provide a copy of the notice to TRICARE beneficiaries upon request. The Military Health System will maintain a current notice on the TRICARE web site at
http://www.tricare.osd.mil. The contractor shall maintain a link to the MHS Notice of Privacy Practices on their web site. The TMA Privacy Officer is responsible for notice maintenance.

5.7. Business Associate Contracts

5.7.1. TMA considers the contract between TMA and the contractor a business associate relationship. Paragraph 5.0., satisfies the requirements of §164.504(e).

5.7.2. The contractor shall ensure that all subcontractors or agents to whom it provides or receives protected health information, agree to the same restrictions and conditions that apply to the contractor with respect to such information.

5.7.3. The contractor shall use and disclose protected health information for the proper management and administration and to carry out the legal responsibilities of the contractor. The contractor may disclose the information received by them in this capacity if:

- The disclosure is required by law; or
- The contractor obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further

disclosed only as required by law or for the purpose for which it was disclosed to the person; and

- The person notifies the contractor of any instances of which it is aware when the confidentiality of the information has been breached.

5.7.4. The contractor shall not use or further disclose the protected health information other than as permitted or required by this section, or as required by the DoD Health Information Privacy Regulation or the HHS Privacy *Rule* or law.

5.7.5. The contractor shall report to TMA through the Regional Director any use or disclosure of the information not provided for by its contract of which it becomes aware.

5.7.6. The contractor shall make available protected health information in accordance with the HHS Privacy *Rule*, §164.524, the DoD Health Information Privacy Regulation, Chapter 11, and this section of the Operations Manual.

5.7.7. The contractor shall make available information required to provide an accounting of disclosures in accordance with the HHS Privacy *Rule*, §164.528, the DoD Health Information Privacy Regulation, Chapter 13, and this section of the Operations Manual.

5.7.8. The contractor shall make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the contractor on behalf of the TRICARE health plan, available to TMA, or at the request of TMA to the Secretary, for purpose of the Secretary determining the TRICARE health plan's compliance with the HHS HIPAA Privacy *Rule*.

5.7.9. The contractor agrees to mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of protected health information by the them in violation of the requirements of this agreement.

5.7.10. The contractor agrees to provide access, at the request of TMA, and in the time and manner designated by TMA, to protected health information in a designated record set, to TMA or, as directed by TMA, to an individual in order to meet the requirements under the HHS Privacy Regulation §164.524 and the DoD Health Information Privacy *Rule*, Chapter 11.

5.7.11. The contractor agrees to make any amendment(s) to protected health information in a designated record set that TMA directs or agrees to pursuant to the HHS Privacy *Rule*, §164.526, or the DoD Health Information Privacy Regulation, Chapter 12, at the request of TMA or an individual, and in the time and manner designated by TMA.

5.8. Personnel

5.8.1. Personnel Designation

The contractor shall designate a privacy official for the implementation and compliance of the HHS Privacy *Rule* and the DoD Health Information Privacy Regulation. The responsibilities of this position include, as a minimum:

5.8.1.1. Purpose/Function: This position oversees all contract activities related to the development, implementation, maintenance of, and adherence to the contractor's policies and procedures covering the privacy of, and access to, protected health information. In addition, this position ensures compliance with federal and state laws, HIPAA, DoD and TRICARE regulations and the organization's information privacy practices.

5.8.1.2. Ensure accomplishment of the following responsibilities:

- Establish, implement and amend policies and procedures with respect to protected health information (PHI) that are designed to ensure compliance with federal and state laws, DoD and HHS Privacy *Rule* and TMA requirements.
- Maintain current knowledge of applicable federal and state privacy laws.
- Monitor and where feasible adopt industry best practices of PHI technologies and management.
- Serve as a liaison to the Regional Director and TMA.
- Cooperate with TMA, Office of Civil Rights, other legal authorities, and organizational personnel in any compliance reviews or investigations.
- Perform initial and periodic privacy risk assessments and conduct related ongoing compliance monitoring activities as applicable.
- Establish a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions.
- Receive complaints and provide information about the organization's privacy practices. Provide the Regional Director with complaint activity in the agreed upon format.
- Mitigate to the extent practicable, any harmful effects known to the organization from the disclosure of PHI in violation of the organization's policies and procedures or its obligation under the privacy regulation.
- Ensure that a written or electronic copy is maintained for the retention period (six years plus current year) of:
  - All policies and procedures (in addition, all policies and procedures must be retained for 6 years and 3 months from the date the contract is closed),
  - Communications required to be in writing and,
  - Documentation of actions or designations that are required by the regulation to be documented.

- Oversee, direct, and ensure delivery of initial privacy training and orientation to all employees, volunteers, clinical staff, business associates, and other appropriate third parties and record results in compliance with contractor training documentation policies. Ensure periodic refresher training is conducted in order to maintain workforce awareness and to introduce any changes to privacy policies.

- Initiate, facilitate and promote activities to foster information privacy awareness within the organization and related entities.

- Collaborate with other departments and subcontractors to continue to ensure appropriate administrative, technical, physical and security safeguards are in place to protect the privacy of PHI.

- Work cooperatively with all applicable organizational units and subcontractors in overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate.

5.9. Documentation

5.9.1. Policies And Procedures

The contractor shall document, implement and maintain policies and procedures required to comply with the HHS Privacy *Rule* and the DoD Health Information Privacy Regulation. These policies and procedures shall be made available upon government request. The contractor shall develop or update their policies and procedures to include, for example, the following:

- Minimum necessary rule.

- Verifying identity of persons seeking disclosure.

- Identify circumstances when the entire medical record is needed.

- Disclosure accounting documentation.

- All Privacy complaints received and their disposition.

- To cooperate and coordinate with HHS Secretary and OCR when investigating privacy violations.

- The name and title of the privacy official and contact person or office who is responsible for receiving complaints and requests for access and amendments by individuals.

- Training requirements.

- Sanctions imposed against non-complying workforce members.

- Whistle-blower provisions.

- Personal Representatives including deceased individuals and abuse, neglect and endangerment situations.
- Providing an individual access to their protected health information, except for those instances identified at paragraphs 2.3.3.1. and 2.3.3.2.
- Providing an individual the right to request restrictions of uses and disclosures of their protected health information to carry out treatment, payment, and healthcare operations; and disclosures to family and friends involved in the patient's care. All restriction requests must be submitted in writing.
- Restriction terminations.
- Providing individuals the right to receive confidential communications.
- Providing individuals the right to request amendment of protected health information.
- Performing initial and periodic information privacy risk assessments and conducting related ongoing compliance monitoring activities, as applicable.
- Safeguarding protected health information from intentional or unintentional misuse.
- Authorizations, including revocation procedures.

5.9.2. Protected Health Information Record Retention

The contractor shall retain all documentation, files, and records related to protected health information in accordance with Chapter 2.

5.10. Safeguards

The contractor shall have in place administrative, technical, and physical safeguards to protect the privacy of protected health information in all forms, including electronic communications, oral communications and paper formats. The safeguards shall be in accordance with Chapter 1, Section 5, paragraph 4.3. and the DoD Privacy Regulation, DoD 5400.11-R, Chapter 1, paragraph D., regarding safeguarding an individual's protected health information applicable for compliance with the Privacy Act of 1974.

5.11. Regional Director/MTF And Contractor Interfaces

5.11.1. Resource sharing/support is considered a covered function of treatment, payment and health care operations by the HHS Privacy *Rule*. The contractor, as a business associate, is subject to the HHS Privacy *Rule* and the DoD Health Information Privacy Regulation when conducting resource sharing functions as outlined in Chapter 16.

5.11.2. The contractor shall develop, document and incorporate into its resource sharing/support program functions policies and procedures ensuring compliance with the DoD Health Information Privacy Regulation and the HHS Privacy *Rule*.

5.11.3. The contractor shall require resource sharing/support providers to use the MHS Notice of Privacy Practices and HHS Privacy *Rule* compliant authorization forms, when applicable.

5.11.4. The contractor shall coordinate with the appropriate Regional Director to determine how they may assist the Military Health System with dissemination of the Notice of Privacy Practices to applicable TRICARE beneficiaries whenever there is a material revision to the MHS Notice of Privacy Practices.

5.11.5. The contractor shall forward initial privacy risk assessments, and the accompanying action plan to the Contracting Officer (CO) with copies to the Regional Director, the Administrative Contracting Officer (ACO), and the Contracting Officer Representative (COR), and the TMA Privacy Officer for review and monitoring of compliance (see paragraph 5.1.).

5.11.6. The contractor shall forward an annual letter of assurance (Chapter 24, Addendum C, Figure 24-C-2) to the Regional Director, with copies to the Contracting Officer (CO), the Administrative Contracting Officer (ACO), and the Contracting Officer Representative (COR), and the TMA Privacy Officer (see paragraph 5.1.2.).

5.11.7. The contractor shall forward all requests for non-routine disclosures, which are any disclosures outside permitted disclosures of protected health information for treatment, payment, and healthcare operations, through the Regional Director to the TMA Privacy Officer (see paragraph 5.2.1.2.).

5.11.8. The contractor shall provide a copy of all amendment response extensions to the Regional Director (see paragraph 5.2.6.2.).

5.11.9. The contractor shall document receipt of all access requests using a date stamp and maintain an index to record pertinent information and actions. If the contractor decides they will not grant access to the protected health information or the record, they shall forward the request within seven working days from receipt of the request to the Regional Director (see paragraph 5.2.4.).

5.11.10. The contractor shall forward a monthly report to the Regional Director, which identifies the beneficiary's name, sponsor's social security number, nature of the complaint, the steps taken to resolve the complaint, the date of the initial complaint, and the expected date of resolution or the date the complaint was resolved (see paragraph 5.4.2.).